CLAIMS

What is claimed is:

1. A computer implemented method comprising:

encrypting a consumer contact information to generate an encrypted value of the consumer contact information;

comparing the encrypted value of the consumer contact information against a master do-not-contact list, the master do-not-contact list comprising a plurality of contact information of a plurality of consumers that have been encrypted; and

determining that the consumer should not be contacted if the encrypted value of the consumer contact information matches one of the plurality of contact information of a plurality of consumers that have been encrypted in the master do-not-contact list.

2. The method as in claim 1 wherein the encrypting further comprises performing a one-way hash of the consumer contact information to generate a hashed value of the consumer contact information, wherein the plurality contact information of the plurality of consumers that have been encrypted includes a plurality of one-way hashed values of the contact information of the plurality of consumers, and wherein the determining includes determining that the consumer should not be contacted if the hashed value of the consumer contact information matches one of the plurality of one-way hashed values in the master do-not-contact list.

3. The method as in claim 1 further comprising:

collecting the consumer contact information using a data collection system

4. The method as in claim 1 further comprising:

causing the consumer contact information to be at least one of automatically purged from a contact list, purged from a client's machine, blocked from entering a contact list, and reported that the consumer contact information is on the master do-not-contact list.

5. The method as in claim 1 wherein the consumer contact information includes at least one of an email address, a user identifier, a domain name, an instant message identifier, a telephone number, and an information that identifies an individual communication device or account.

6. The method as in claim 1 wherein the consumer contact information includes demographic information or a category of a set of entries fitting a particular characteristic.

7. A computer implemented method comprising:

collecting a set of one or more do-not-contact list entries, each do-not-contact list entry is a string of characters representing a consumer

contact information;

applying a one-way hashing scheme to the set of one or more do-not-contact list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-contact list entries;

transferring the set of one or more hashed do-not-contact list entries to a master do-not-contact list server configured to store the set of one or more hashed do-not-contact list entries; and

comparing an encrypted client entry against the set of one or more hashed do-not-contact list entries.

8. The method as in claim 7 wherein the encrypted client entry is a hashed value of a contact information stored on a client machine, the client machine is communicable with the master do-not-contact list server to check if the contact information appears in the set of one or more hashed do-not-contact list entries.

9. The method as in claim 8 wherein the comparing of the encrypted client entry against the set of one or more hashed do-not-contact list entries allows the client machine to protect the contact information.

10. The method as in claim 8 wherein the encrypted client entry is created on the client machine and wherein the contact information is both stored and

hashed on the client machine.

11. The method as in claim 8 wherein the comparing of the encrypted client entry against the set of one or more hashed do-not-contact list entries is performed on the client machine.

12. The method as in claim 7 configuring a master do-not-contact list database to be in communication with the master do-not-contact list server, the master do-not-contact list database configured to store the set of one or more hashed do-not-contact list entries for the master do-not-contact list server.

13. A computer implemented method comprising:

collecting a set of one or more do-not-contact list entries, each do-not-contact list entry is a string of characters representing a contact information;

applying a one-way hashing scheme to the set of one or more do-not-contact list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-contact list entries;

transferring the set of one or more hashed do-not-contact list entries to a master do-not-contact list server configured to store the set of one or more hashed do-not-contact list entries;

requesting from the master do-not-contact list server at least one hashed do-not-contact list entry from the set of one or more hashed do-not contact list entries to create or update a client do-not-contact list on a client machine;

causing a client entry to be hashed to create a hashed client entry; and

comparing the hashed client entry to the client do-not-contact list to determine whether the client entry appears on the client do-not-contact list.

14. The method as in claim 13 wherein the hashed client entry is a hashed value of a contact information stored on the client machine, the client machine performs the causing of the client entry to be hashed, the client machine performs the requesting from the master do-not-contact list server, and the client machine performs the comparing the hashed client entry to the client do-not-contact list.

15. The method as in claim 13 wherein the hashed client entry is a hashed value of a contact information stored on the client machine and the client machine performs the causing of the client entry to be hashed.

16. The method as in claim 13 configuring a master do-not-contact list database to be in communication with the master do-not-contact list

server, the master do-not-contact list database configured to store the set of one or more hashed do-not-contact list entries for the master do-not-contact list server.

17. The method as in claim 14 wherein the comparing of the hashed client entry against the set of one or more hashed do-not-contact list entries allows the client machine to protect the contact information.

18. The method as in claim 13 wherein the contact information includes demographic information, and wherein the client entry includes the demographic information.

19. The method as in claim 13 wherein the contact information includes demographic information, wherein the client entry includes the demographic information, and wherein the comparing the hashed entry to the client do-not-contact list to includes determining that consumers having the demographic information wish to not be contacted when the client entry appears on the client do-not-contact list.

20. A computer implemented method comprising:

performing a one-way hash of an email address to generate a hashed value of the email address;

comparing the hashed value of the email address against a master

do-not-email list, the master do-not-email list comprising a plurality of one-way hashed values of a set of one or more email addresses of a one or more individuals; and

determining that the individual should not be contacted if the hashed value of the email address matches one of the one-way hashed values of the set of one or more email addresses.

21. The method as in claim 20 further comprising:

collecting the email address using a data collection system

22. The method as in claim 20 further comprising:

causing the email address to be at least one of automatically purged from a contact list, purged from a client's machine, blocked from entering a contact email list, blocked from entering a spam list, purged from a spam list, and reported that the email address is on the master do-not-contact list.

23. A computer implemented method comprising:

collecting a set of one or more do-not-email list entries, each do-not-email list entry is a string of characters representing an email address;

applying a one-way hashing scheme to the set of one or more do-not-email list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-email list

entries;

transferring the set of one or more hashed do-not-email list entries to a master do-not-email list server configured to store the set of one or more hashed do-not-email list entries; and

comparing an encrypted client entry against the set of one or more hashed do-not-email list entries.

24. The method as in claim 23 wherein the encrypted client entry is a hashed value of an email address stored on a client machine, the client machine is communicable with the master do-not-email list server to check if the email information appears in the set of one or more hashed do-not-email list entries.

25. The method as in claim 24 wherein the comparing of the encrypted client entry against the set of one or more hashed do-not-email list entries allows the client machine to protect the email address.

26. The method as in claim 24 wherein the encrypted client entry is created on the client machine and wherein the email address is both stored and hashed on the client machine.

27. The method as in claim 24 wherein the comparing of the encrypted client entry against the set of one or more hashed do-not-email list entries is

performed on the client machine.

28. The method as in claim 23 configuring a master do-not-email list database to be in communication with the master do-not-email list server, the master do-not-email list database configured to store the set of one or more hashed do-not-email list entries for the master do-not-email list server.

29. A computer implemented method comprising:

collecting a set of one or more do-not-email list entries, each do-not-email list entry is a string of characters representing an email address;

applying a one-way hashing scheme to the set of one or more do-not-email list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-email list entries;

transferring the set of one or more hashed do-not-email list entries to a master do-not-email list server configured to store the set of one or more hashed do-not-email list entries;

requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a client do-not-email list on a client machine;

causing a client email entry to be hashed to create a hashed client email entry; and

comparing the hashed client email entry to the client do-not-email list to determine whether the hashed client email entry appears on the client do-not-email list.

30. The method as in claim 29 wherein the hashed client email entry is a hashed value of an email address stored on the client machine, the client machine performs the causing of the client email entry to be hashed, the client machine performs the requesting from the master do-not-email list server, and the client machine performs the comparing the hashed client email entry to the client do-not-email list.

31. The method as in claim 29 wherein the hashed client email entry is a hashed value of an email address stored on the client machine and the client machine performs the causing of the client email entry to be hashed.

32. The method as in claim 29 configuring a master do-not-email list database to be in communication with the master do-not-email list server, the master do-not-email list database configured to store the set of one or more hashed do-not-email list entries for the master do-not-email list server.

33. The method as in claim 30 wherein the comparing of the hashed client entry against the set of one or more hashed do-not-email list entries allows the client machine to protect the email address.

34. The method as in claim 29 wherein the requesting from the master do-not-email list server of at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update the client do-not-email list on the client machine is maintained by an email marketer.

35. The method as in claim 34 wherein the email marketer uses a client do-not-email list application to cause the requesting from the master do-not-email list server and to create or update the client do-not-email list on the client machine.

36. The method as in claim 35 wherein the email marketer uses the client do-not-email list application to periodically check bulk email lists maintaining by the email marketer to have email addresses associated with the set of one or more do-not-email list entries be kept free of spam.

37. A non-revealing do-not-contact system comprising:

a do-not-contact list client application communicable with a master do-not-contact list server configured to provide retrieval of unique hashed values, each unique hashed value associates with a consumer contact information;

a client do-not contact list created by at least partially by the

retrieval of at least one the unique hashed values provided by the master do-not-contact list server;

a client machine to maintain or operate the do-not contact list client application; and

a comparison scheme to compare a hashed client entry to the client do-not-contact list.

38. The system as in claim 37 wherein a master do-not-contact list database communicable with the master do-not-contact list server is used to store the unique hashed values for the master do-not-contact list server.

39. The system as in claim 37 wherein the consumer contact information is collected by a data collection system, wherein the data collection system transfers the consumer contact information to a one-way hash engine that converts the consumer contact information into a unique hashed value.

40. The system as in claim 37 wherein each unique hash value associates with consumer demographic information which includes the consumer contact information and wherein the hashed client entry associates with consumer demographic information.

41. The system as in claim 39 wherein the do-not-contact list client application retrieves at least one of the hashed values or additional updates from the

master-do-not contact list server through at least one of a network connection, an email, a disk, and a scanned form.

42. The system as in claim 39 wherein the consumer contact information is sorted by demographic information.

43. The system as in claim 42 wherein the demographic information includes at least one of legal jurisdiction that applies to the consumer, minor/adult status that applies to the consumer, types of messages that the consumer allows and not allows, and type of one-way hashing scheme.

44. The system as in claim 39 wherein the one-way hash engine uses at least one hashing scheme selected from a group consisting of SHA-0, SHA-1, SHA-256, SHA-384, SHA-512, MD2, MD4, MD5, RIPEMD-160, RIPEMD-128/256/320, HAS160, HAS-V, HAVAL, Tiger, Panama, Snefru-2, GOST-Hash, BRS-H1/H20, and Whirpool.

45. The system as in claim 37 wherein the client machine performs the comparison scheme that compares the hashed client entry to the client do-not-contact list.

46. The system as in claim 37 wherein the hashed client entry represents a client consumer contact information entered into the client machine,

wherein the client machine performs a hash on the client consumer contact information to create the hashed client entry.

47. The system as in claim 46 wherein the client machine uses at least one hashing scheme selected from a group consisting of SHA-0, SHA-1, SHA-256, SHA-384, SHA-512, MD2, MD4, MD5, RIPEMD-160, RIPEMD-128/256/320, HAS160, HAS-V, HAVAL, Tiger, Panama, Snefru-2, GOST-Hash, BRS-H1/H20, and Whirpool.

48. The system as in claim 37 wherein the do-not-contact list client application is deployed on multiple remote computers of at least one of individuals, businesses, and clients, that send unsolicited communications or store or use the consumer contact information.

49. A non-revealing do-not-contact system comprising:

a client application communicable with a master do-not-contact list server, the client application capable of sending a hashed client entry to the master do-not-contact list server, the hashed client entry representing a client consumer contact information that is converted into a unique hashed value bearing seemingly no resemblance to the client consumer contact information, the master do-not-contact list server providing retrieval of at least one hashed value, each representing a consumer contact information;

a client machine to maintain or operate the client application to

send the hashed client entry; and

a comparison scheme to compare the hashed client entry against the at least one hashed value retrieved through the master do-not-call list server.

50. The system as in claim 49 wherein the master do-not-contact list server provides the retrieval of the at least one hashed value through a master do-not-contact list database.

51. The system as in claim 49 wherein the consumer contact information is collected by a data collection system, wherein the data collection system transfers the consumer contact information to a one-way hash engine that converts the consumer contact information into the hashed value.

52. The system as in claim 51 wherein the consumer contact information is sorted by demographic information.

53. The system as in claim 52 wherein the demographic information includes at least one of legal jurisdiction that applies to the consumer, minor/adult status that applies to the consumer, types of messages that the consumer allows and not allows, and types of one-way hashing scheme.

54. The system as in claim 51 wherein the one-way has engine includes at least

one one-way hashing scheme being selected from a group consisting of SHA-0, SHA-1, SHA-256, SHA-384, SHA-512, MD2, MD4, MD5, RIPEMD-160, RIPEMD-128/256/320, HAS160, HAS-V, HAVAL, Tiger, Panama, Snefru-2, GOST-Hash, BRS-H1/H20, and Whirpool.

55. The system as in claim 49 wherein the client machine performs the comparison scheme that compares the hashed client entry to the at least one hashed value retrieved through the master do-not-contact list server.

56. The system as in claim 49 further comprises a one-way hash engine communicable with the client machine to hash the client consumer contact information to create the hashed client entry.

57. The system as in claim 56 wherein the one-way has engine includes at least one one-way hashing scheme being selected from a group consisting of SHA-0, SHA-1, SHA-256, SHA-384, SHA-512, MD2, MD4, MD5, RIPEMD-160, RIPEMD-128/256/320, HAS160, HAS-V, HAVAL, Tiger, Panama, Snefru-2, GOST-Hash, BRS-H1/H20, and Whirpool.

58. The system as in claim 49 further comprises a one-way hash engine coupling to or residing within the client machine to hash the client consumer contact information to create the hashed client entry.

59. A method comprising:

causing a consumer contact information to be hashed by a one-way hash engine to convert the consumer contact information into a hashed client contact entry;

causing the hashed client contact entry to be compared against a client do-not-contact list wherein the client do-not-contact list is created at least partially by using hashed values retrieved through a master do-not-contact list server, the hashed values representing a set of one or more contact information of consumers who do not wish to be contacted; and

determining that the consumer with the consumer contact information is not to be contacted when the hashed client contact entry matches anyone of the hashed values retrieved through the master do-not-contact list server.

60. The method as in claim 59 wherein the consumer contact information is collected by a client machine and is hashed by the one-way hash engine connected to the client machine.

61. The method as in claim 59 wherein the consumer contact information is collected by a client machine, hashed by the one-way hash engine residing in the client machine, and compared to the hashed values retrieved through the master do-not-contact list server on the client machine.

62. The method as in claim 59 further comprises causing the contact information of consumers to be collected by a data collection system, hashed by a second one-way hash engine communicable with the data collection system, and transferred to the master do-not-contact list server.

63. The method as in claim 62 further comprises causing a master do-not-contact list server communicable with the master do-not-contact list server to store the hashed values.

64. The method as in claim 59 further comprises causing a do-not-contact list client application to be in communication with the master do-not-contact list server to retrieve at least one hashed value from the master-do-not contact list server to create the client do-not-contact list.

65. The method as in claim 59 further comprises causing the one-way has engine to include at least one one-way hashing scheme being selected from a group consisting of SHA-0, SHA-1, SHA-256, SHA-384, SHA-512, MD2, MD4, MD5, RIPEMD-160, RIPEMD-128/256/320, HAS160, HAS-V, HAVAL, Tiger, Panama, Snefru-2, GOST-Hash, BRS-H1/H20, and Whirpool.

66. The method as in claim 62 further comprises causing the data collection system to specify at least one one-way hashing scheme to be applied to the

entries collected by the data collection system.

67. A computer implemented method to identify email addresses registered on a do not contact list that are in a client's list without revealing the email addresses on the do not contact list or the client's list comprising:

the client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address;

the client transmitting over a network said plurality of encrypted entries from the client's list to a service for comparison to encrypted entries of the do not contact list, wherein the encrypted entries of the do not contact list were formed by encrypting information, including at least an email address, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the do-not-contact list represents that the underlying email address needs to be identified; and

the client receiving results of the comparison.

68. The computer implemented method of claim 67, wherein the client receiving results of the comparison comprises:

the client receiving back information identifying only those of said transmitted encrypted entries that matched.

69. The computer implemented method of claim 67, wherein the client

receiving results of the comparison comprises:

the client receiving back information identifying only those of said transmitted encrypted entries that did not match.

70. The computer implemented method of claim 67, further comprising:

the client determining which entries on the client's list matched based on said received results; and

the client removing the matched entries from the client's list.

71. A computer implemented method to identify email addresses registered on a do-not-contact list that are in a client's list without revealing the email addresses on the do-not-contact list or the client's list comprising:

the client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address;

the client transmitting over a network said plurality of encrypted entries from the client's list to a service for comparison to encrypted entries of the do-not-contact list, wherein the encrypted entries of the do-not-contact list were formed by encrypting information, including at least an email address that belongs to a minor, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the do-not-contact list represents that the underlying email address needs

to be identified; and

the client receiving results of the comparison.

72. The computer implemented method of claim 71, wherein the encrypted entry belonging to the minor is automatically removed from the client's list.

73. The computer implemented method of claim 71, further comprising:

associating the email address that belongs to the minor with a parent's address.

74. The computer implemented method of claim 73, further comprising:

the client causing a notification to be sent to the parent 's address to notify the parent when there is a request to remove the contact information associating with the encrypted entry that belongs to the minor from the do-not-contact list.

75. The computer implemented method of claim 73, further comprising:

the client causing a notification to be sent to the parent 's address to notify the parent when there is an attempt to remove the contact information associating with the encrypted entry that belongs to the minor from the do-not-contact list.

76. The computer implemented method of claim 71, wherein the client receiving results of the comparison comprises:

the client receiving back information identifying only those of said transmitted encrypted entries that matched.

77. The computer implemented method of claim 71, wherein the client receiving results of the comparison comprises:

the client receiving back information identifying only those of said transmitted encrypted entries that did not match.

78. The computer implemented method of claim 71, further comprising:

the client determining which entries on the client's list matched based on said received results; and

the client removing the matched entries from the client's list.

79. A computer implemented method to identify email addresses registered on a do-not-contact list without revealing the email addresses on the do-not-contact list comprising:

a client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address that does not wish to be contacted;

the client causing a comparison of said plurality of encrypted entries from the client's list to a plurality of encrypted entries of a master

do-not-contact list, wherein the encrypted entries of the master do-not-contact list were formed by encrypting information, including at least an email address that belongs to a minor, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the master do-not-contact list represents that the underlying email address needs to be identified;

the client receiving results of the comparison; and

the client updating the client's list with encrypted information retrieved from the master do-not-contact list.

80. The computer implemented method of claim 79, wherein when the encrypted entry that matches one of the encrypted entries of the master do-not-contact list of belongs to the minor is automatically removed from the client's list.

81. The computer implemented method of claim 79, further comprising:

associating the email address that belongs to the minor with a parent's address.

82. The computer implemented method of claim 81, further comprising:

the client causing a notification to be sent to the parent 's address to notify the parent when there is a request to remove the contact information associating with the encrypted entry that belongs to the minor from the

client's list

83. A method of protecting a master do-not-contact list, the method including:

including a false record in the master do-not-contact list;

implanting the false record into a client do-not-contact list;

monitoring to see if a contact information associating with the false record is used and sent to a false server configured to receive the contact information.

84. The method of claim 83 wherein the master do-not-contact list includes a master-do-not-email list, wherein the false record includes a false email address that points to an email account not used for any real email, and wherein the false server includes a false email server configured to receive an email addressed associated with the false email address.

85. The method of claim 83 further comprises causing an investigation into a client that uses the false record.

86. A computer implemented method comprising:

providing a non-revealing do-not-contact list of one-way hashed consumer contact information to a set of one or more entities for the set of entities to determine whether certain consumers do not wish to be

contacted without discovering actual consumer contact information.

87. A computer implemented method comprising:

encrypting a category of consumer information to generate an encrypted value of the category of consumer information;

comparing the encrypted value of the category of consumer information against a master do-not-contact list, the master do-not-contact list comprising a plurality of categories of consumer information for a plurality of categories of consumers, the plurality of categories of consumer information encrypted; and

determining that the category of consumer information should not be contacted if the encrypted value of the category consumer information matches one of the plurality of categories of consumer information in the master do-not-contact list.

88. The method of claim 87 wherein the category of consumer information includes any one of youth, elderly, age group, nationality, gender, ethnicity, area, city, town, state, county, country, area code, zip code, email address, email provider, internet service provider, school email address provider, library email address provider, and government sector email address.